Doc Code: AP.PRE.REQ

PTO/SB/33 (08-08)
Approved for use through 08/31/2008. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional)
50325-0865

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]

on February 25, 2009

Signature /KarlTRees#58983/

Typed or printed name Karl T. Rees

Application Number	Filed
10/797,773	March 9, 2004
First Named Inventor	
Mark Ammar Rayes	
Art Unit	**Examiner**
2434	Shaifer Harriman, Dant B

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

- ☐ applicant/inventor.
- ☐ assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)
- ☑ attorney or agent of record. Registration number 58,983.
- ☐ attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34 _____

/KarlTRees#58983/
Signature

Karl T. Rees
Typed or printed name

(408) 414-1080
Telephone number

February 25, 2009
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☑ *Total of 1 forms are submitted.

This collection of information is required by 35 U.S.C. 132. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Mark Ammar Rayes, et al.	)	Group Art Unit No.: 2434
	)	Examiner: Shaifer Harriman, Dant B
Serial No.: 10/797,773	)	
	)	Confirmation No.: 4164
Filed on: March 9, 2004	)	
	)	
For: ISOLATION APPROACH FOR NETWORK USERS ASSOCIATED WITH ELEVATED RISK	)	

Mail Stop AF, Pre-Appeal Conference
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

ATTACHMENT TO PRE-APPEAL BRIEF REQUEST FOR REVIEW

REMARKS/ARGUMENTS

I. STATUS OF CLAIMS

Claims 1–13, 18–20, 30–38, and 43–44 are pending. Claims 1–13, 18–20, 30–38, and 43–44 stand rejected under 35 U.S.C. §103(a) as allegedly unpatentable over U.S. 7,194,004 B1 ("*Thomsen*"), in view of U.S. 7,127,524 B1 ("*Renda*").

II. THE REJECTIONS ARE BASED ON CLEAR FACTUAL ERRORS

The rejection set forth the Final Office Action of November 28, 2008 ("Office Action") is based on a factually erroneous understanding of *Thomsen* and the pending claims. For example, the rejection is based on at least the clear factual errors discussed in the following sections.

A. CLAIM 1

1. *Thomsen* moves devices from an untrusted network to a trusted network—the opposite of Claim 1

Claim 1 recites a method for moving a device that has caused a security event from a "first network address assigned **from** a first subset of addresses within a first specified pool associated with **normal network users**" **to** a "a second network address that is selected from a

second subset of addresses within a second specified pool associated with **suspected malicious network users**."

By contrast, *Thomsen* describes a process whereby a device is initially assigned to an untrusted network and then moved to a trusted network once the device is authenticated. *Thomsen* at col. 5, lines 61–65. This process is almost exactly opposite to that described in Claim 1, as illustrated in the table below.

	Claim 1	*Thomsen*
Initial Network Address	"first network address assigned from a first subset of addresses within a first specified pool associated with **normal network users**"	"assigned to an **untrusted subnet**"
Network Address after alleged security event	"second network address that is selected from a second subset of addresses within a second specified pool associated with **suspected malicious network users**"	"assigned to a **trusted subnet**"

Despite these clear differences, the Office Action nonetheless alleges that *Thomsen*'s technique is the same as that of Claim 1. *Office Action* at 8. The Office Action is clearly factually erroneous. One skilled in the art would never confuse a "pool associated with normal network users" with a "untrusted subnet." Neither would one skilled in the art consider a "trusted subnet" to be a "pool associated with suspected malicious network users."

In fact, *Thomsen*'s techniques are directed towards a very different problem that the method of Claim 1. Whereas *Thomsen* is concerned with how to move an unknown user on to a trusted network, Claim 1 is concerned with how to deal with a user who, while on a "normal network," causes a security event. The matter does not involve "interpreting" *Thomsen* or the claims, as the plain meaning of the claim terms and a straightforward reading of *Thomsen* establishes that the approaches are entirely different. Accordingly, *Thomsen*'s techniques would not have taught or suggested any aspect of Claim 1 to one skilled in the art.

2. *Thomsen* only assigns a new address if there is no alleged "security event;"
Claim 1 assigns a new address in response to a security event

Even if *Thomsen* could somehow be construed to as relevant to a nearly opposite technique, *Thomsen* still fails to teach or suggest the Claim 1's recited feature of "in response to

[a] security event [caused by a network device], causing the network device to acquire a second network address." The Office Action nonetheless alleges that *Thomsen* teaches such a step because a device on an un-trusted network is assigned an IP address for a trusted network upon authentication. *Office Action* at 8, 11. Moreover, the Office Action alleges that the "security event" in response to which the new address is assigned is an "authentication failure." *Office Action* at 11. The Office Action is clearly factually erroneous.

Thomsen does not teach that, in response to the alleged security event—i.e. the authentication failure—one should reassign a device having an address on an un-trusted network to an address on a trusted network. Rather, the only address assignment that occurs in response to *Thomsen*'s authentication failure is the assignment of a device having no address to an address at an un-trusted network. *Thomsen* at col. 5, lines 58–59. Clearly, this is different than Claim 1's recited response strategy of reassigning a device that already has a first address to a second address.

In fact, the only occasion upon which *Thomsen* assigns a new address to a device already having an address is a successful authentication—in other words, the lack of the alleged security event. Nor would it be obvious to modify *Thomsen* to reassign the address of a device that already had an address in response to an authentication failure—if the device were already assigned an address on the un-trusted network, there would of course be no reason to reassign that device to the un-trusted network.

Perhaps the Office Action intends to allege that a successful "authentication"—and not an "authentication failure"—is the security event in response to which address reassignment occurs. Even so, the Office Action would still be in clear error for at least the reason that a successful authentication does not "indicate[] at least one of: a possible denial of service attack, possible IP address spoofing, extraneous requests for network addresses, and possible MAC address spoofing," and therefore is not a security event within the meaning of Claim 1.

3. The Office Action is inconsistent in its allegations concerning what aspect of *Thomsen* corresponds to a security event

The Office Action alleges on page 7 that *Thomsen*'s "IP address spoofing" is the security event of Claim 1 in the context of Claim 1's feature of "wherein the security event is an event that indicates at least one of: a possible denial of service attack, possible IP address spoofing,

extraneous requests for network addresses, and possible MAC address spoofing." Yet the Office Action later alleges on page 11 that *Thomsen*'s authentication failure is the security event of Claim 1 in the context of Claim 1's feature of "in response to the security event, causing the network device to acquire a second network address." The Office Action is internally inconsistent; no skilled artisan would read *Thomsen* with such an inconsistency. No single element in *Thomsen* can be understood to correspond to the "security event" recited in both of the above-quoted features of Claim 1. The Office Action is thus factually erroneous in its allegations that *Thomsen* teaches the security event of Claim 1.

B. CLAIM 3

Claim 3 recites "resetting a port that is coupled to the network device to prompt a user to command the network device to request a new network address using DHCP" as a technique for forcing normal users on to a network for suspected malicious users. The Office Action alleges that one way to "reset a port" is for "a new device with a different IP address start to communicate with the port." The Office Action is clearly erroneous.

The Office Action apparently does not understand the meaning of the word "port," as understood by one skilled in the art. A port is an "interface between the computer and other computers or peripheral devices." *E.g.* http://en.wikipedia.org/wiki/Computer_port_(hardware). It is not possible to reset a port by "a new device with a different IP address start to communicate with the port." Rather, one must perform some action that actually interrupts the connection to the port. *Thomsen* does not teach the use of such a step to force normal users on to a network for suspected malicious users.

C. CLAIM 4

Claim 4 recites the use of a "DHCP_FORCE_RENEW message" as a technique for forcing normal users on to a network for suspected malicious users. The Office Action alleges that the use of such a message is taught in *Thomsen* at col. 8, lines 12–14, col. 10, lines 62–64, and col. 11, lines 56–60. The Office Action is clearly factually erroneous. There is absolutely no mention of such a message in any passage of *Thomsen*.

D. CLAIM 12

Claim 12 recites the method of Claim 1 with an additional step of "determining whether a malicious act caused the security event, and if not, removing the user from the second specified

pool." Although Applicants disagree that *Thomsen* teaches or is even equipped to "determine[e] whether a malicious act caused the [alleged] security event," it is at a minimum clear that *Thomsen* does not contemplate that a user, having already been shifted from a first pool to a second pool, would then be removed from that second pool. *See* Applicants' Response of July 14, 2008 at 19.

E. THE REMAINING CLAIMS

All pending claims not discussed above either depend from, or recite features similar to, the claim features discussed above. Therefore, for at least one or more of the same reasons discussed above, the rejection as to these remaining pending claims is based on one or more clear factual errors.

III. CONCLUSION

For at least these above reasons, the Office's rejection of each of the pending claims is based on clear factual errors. Moreover, *Renda* does not, nor does the Office Action allege *Renda* to, teach or suggest any of the above discussed features. Because *Renda* does not cure the deficiencies of *Thomsen* in failing to disclose the complete subject matter that is claimed, the Office action fails to state a *prima facie* case of unpatentability. The cited references fail to teach or suggest at least one element of each pending claim. Applicants therefore request that the Office remove the current rejection of the pending claims.

For the reasons set forth above, the pending claims are now in condition for allowance. Applicants respectfully request that the Office withdraw the rejections and allow the claims.

Respectfully submitted,
HICKMAN PALERMO TRUONG & BECKER LLP

Date: February 25, 2009 /KarlTRees#58983/
Karl T. Rees, Reg. No. 58,983

2055 Gateway Place, Suite 550
San Jose, CA 95110
Voice: (408) 414-1233
Facsimile: (408) 414-1076